Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (previously presented): A method for managing file security attributes by a file server in a computer file storage system, the computer file storage system including a file secured using a first file security model, the method comprising:

receiving a first request from a client relating to the file stored in the computer file storage system, the client utilizing a second file security model;

retrieving a first set of file security attributes, in accordance with the first file security model, associated with the file, the first set of file security attributes including at least an owner identifier and a group identifier; and

generating a second set of file security attributes, in accordance with the second file security model, from the first set of file security attributes, the second set of file security attributes including a plurality of security identifiers (SID) including at least an owner SID derived from the owner identifier and a group SID derived from the group identifier, wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier from the first set of file security attributes, wherein the map failure indicator indicates that said identifier relates to the first file security model.

Claim 2 (previously presented): A method according to claim 1, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, and an owner/group indicator having a first value to indicate that the identifier is the owner identifier from the first set of security attributes, and a second value to indicate that the identifier is the group identifier from the first set of security attributes.

Claim 3 (previously presented): A method according to claim 1, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 4 (previously presented): A method according to claim 1, wherein generating the second set of file security attributes from the first set of file security attributes comprises:

attempting to map each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes; and

generating, for each identifier from the first set of file security attributes that cannot be mapped to a corresponding identifier from the second set of file security attributes, the SID including the at least one map failure indicator and the corresponding identifier from the first set of file security attributes.

Claim 5 (previously presented): A method according to claim 4, wherein attempting to map each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes comprises:

maintaining a table mapping a first set of names in accordance with the first file security model to a second set of names in accordance with the second file security model;

determining a name from the first set of names corresponding to the identifier from the first set of file security attributes; and

searching the table for a name from the second set of names corresponding to the name from the first set of names.

Claim 6 (previously presented): A method according to claim 5, wherein determining a name from the first set of names corresponding to the identifier from the first set of file security attributes comprises:

maintaining a cache mapping identifiers from the first set of file security attributes to names in the first set of names; and

searching the cache for a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 7 (previously presented): A method according to claim 5, wherein determining a name from the first set of names corresponding to the identifier from the first set of file security attributes comprises:

sending the identifier from the first set of file security attributes over a communication link to a NIS server; and

receiving the name from the first set of names over the communication link from the NIS server.

Claim 8 (previously presented): A method according to claim 1, further comprising:

transmitting the second set of file security attributes to the client in a response to the first request.

Claim 9 (previously presented): A method according to claim 8, further comprising:

receiving a second request from the client utilizing the second file security model including at least one of said SIDs including at least one map failure indicator and the corresponding identifier from the first set of file security attributes;

translating the at least one of said SIDs into a text string; and

transmitting the text string to the client in a response to the second request.

Claim 10 (previously presented): A method according to claim 9, wherein the text string includes a representation of the identifier from the SID.

Claim 11 (previously presented): A method according to claim 1, wherein the first set of file security attributes includes a first set of file permissions, in accordance with the first file security model, and wherein generating the second set of file security attributes from the first set of file security attributes further comprises:

generating a second set of file permissions, in accordance with the second file security model, from the first set of file permissions.

Claim 12 (previously presented): A method according to claim 11, wherein the request comprises at least one requested change to the security attributes of the file, and wherein the method further comprises:

applying the requested security attribute changes to the second set of file security attributes to create a modified set of file security attributes in accordance with the second file security model; and

writing the modified set of file security attributes to the file, said writing effectively changing the security model of the file from the first file security model to the second file security model.

Claim 13 (previously presented): A method according to claim 12, further comprising:

receiving a second request from a client utilizing the first file security model relating to the file, the second request associated with a session, the session having a session owner and a session group;

retrieving the modified set of file security attributes for the file; and

providing the client with owner access to the file, if the owner SID in the modified set of file security attributes includes an owner identifier in accordance with the first file security model and the session owner matches the owner identifier in the owner SID.

Claim 14 (previously presented): A method according to claim 12, further comprising:

receiving a second request from a client utilizing the first file security model relating to the file, the second request associated with a session, the session having a session owner and a session group;

retrieving the modified set of file security attributes for the file; and

providing the client with group access to the file, if the group SID in the modified set of file security attributes includes a group identifier in accordance with the first file security model and the session group matches the group identifier in the group SID.

Claim 15 (previously presented): A method according to claim 11, wherein generating the second set of file permissions from the first set of file permissions comprises:

translating the first set of file permissions into a second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions;

removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone;

adding any rights that need to be explicitly denied to the owner and to the group;

producing a set of access control elements ordered hierarchically; and

removing any redundant permissions from the access control elements.

Claim 16 (previously presented): An apparatus for managing file security attributes in a computer file storage system, the computer file storage system including a file secured using a first file security model, the file associated with a first set of file security attributes including an owner identifier and a group identifier, the apparatus comprising:

a network interface for communicating with clients over a communication network;

a storage interface for communicating with a file storage device; and

file security logic operating between the network interface and the storage interface for managing file security attributes, the file security logic including logic for generating a second set of file security attributes, in accordance with a second file security model, from the first set of file security attributes, the second set of file security attributes including at least an owner SID derived from the owner identifier and a group SID derived from the group identifier, wherein at least one of the owner SID and the group SID includes at least one map failure indicator and the corresponding identifier

from the first set of file security attributes, wherein the map failure indicator indicates that said identifier relates to the first file security model.

Claim 17 (previously presented): An apparatus according to claim 16, wherein the at least one map failure indicator includes an authority identifier, specific to the first security model, and an owner/group indicator having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 18 (previously presented): An apparatus according to claim 16, wherein the at least one map failure indicator includes an authority identifier, specific to the first file security model, having a first value to indicate that the identifier is the owner identifier from the first set of file security attributes and a second value to indicate that the identifier is the group identifier from the first set of file security attributes.

Claim 19 (previously presented): An apparatus according to claim 16, wherein the file security logic comprises:

logic for mapping each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes; and

logic for generating, for each identifier from the first set of file security attributes that cannot be mapped to a corresponding identifier from the second set of file security attributes, the SID including the at least one map failure indicator and the corresponding identifier from the first set of file security attributes.

Claim 20 (previously presented): An apparatus according to claim 19, further comprising a table mapping a first set of names, in accordance with the first file security model, to a second set of names, in accordance with the second file security model, the file security logic determining a name from the first set of names corresponding to the identifier from the first set of file security attributes and searching the table for a name from the second set of names corresponding to the name from the first set of names for

mapping each identifier from the first set of file security attributes to a corresponding identifier from the second set of file security attributes.

Claim 21 (previously presented): An apparatus according to claim 20, further comprising a cache mapping identifiers from the first set of file security attributes to names in the first set of names, the file security logic searching the cache for a name from the first set of names corresponding to the identifier from the first set of file security attributes for determining a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 22 (previously presented): An apparatus according to claim 20, wherein the file security logic sends the identifier from the first set of file security attributes over a communication link to a NIS server for determining a name from the first set of names corresponding to the identifier from the first set of file security attributes.

Claim 23 (original): An apparatus according to claim 16, wherein the file security logic further comprises:

logic for translating the at least one of said SIDs into a text string.

Claim 24 (previously presented): An apparatus according to claim 23, wherein the text string includes a representation of the identifier from the SID.

Claim 25 (previously presented): A method according to claim 16, wherein the first set of file security attributes includes a first set of file permissions, in accordance with the first file security model, and wherein the file security logic further comprises:

logic for generating a second set of file permissions, in accordance with the second file security model, from the first set of file permissions.

Claim 26 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for receiving a request from a client utilizing the second file security model, to modify file security attributes, applying the requested

modifications to the second set of file permissions to create a modified set of file security attributes in accordance with the second file security model, and writing the modified set of file permissions to the storage device so as to effectively change the security model of the file from the first file security model to the second file security model.

Claim 27 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for controlling access to the file using the second set of file permissions.

Claim 28 (previously presented): An apparatus according to claim 25, wherein the file security logic includes logic for translating the first set of file permissions into ~~a~~ the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions; removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone; adding any rights that need to be explicitly denied to the owner and to the group; producing a set of access control elements ordered hierarchically; and removing any redundant permissions from the access control elements.

Claim 29 (previously presented): An apparatus for managing file security attributes in a computer file storage system, the apparatus comprising:

means for translating an owner identifier in accordance with a first file security model into an owner SID, compatible with a second file security model;

means for translating a group identifier in accordance with a first file security model into a group SID, compatible with the second file security model; and

means for translating file access permissions, in accordance with a first file security model, into an access control list, compatible with the second file security model.

Claim 30 (previously presented): A method for generating, from a first set of file permissions in accordance with a first file security model, a second set of file permissions in accordance with a second file security model, the method comprising:

translating the first set of file permissions into the second set of file permissions, the second set of file permissions defining owner permissions, group permissions, and everyone permissions;

removing any rights from the owner that the owner would be granted implicitly but are not granted to either the group or to everyone;

adding any rights that need to be explicitly denied to the owner and to the group;

producing a set of access control elements ordered hierarchically; and

removing any redundant permissions from the access control elements.

Claim 31 (previously presented): A method comprising:

receiving a security identifier (SID) including at least one map failure indicator and a corresponding identifier in accordance with a first file security model; and

translating the SID into a text string.

Claim 32 (previously presented): A method according to claim 31, wherein the text string includes a representation of the identifier from the SID.

Claim 33 (previously presented): A method according to claim 31, wherein translating the SID into a text string comprises:

transmitting a request to a translator over a communication network, the request including at least the identifier from the SID.